International Journal for Housing Science and Its Applications
Publish August 6, 2025. Volume 46, Issue 3 Pages 5871-5881

https://doi.org/10.70517/ijhsa463505

A Framework for Encryption Algorithm-Based Data Security Design and Copyright Protection in Digital Libraries

Peng Xu[1,*]
[1] Library, South-Central Minzu University, Wuhan, Hubei, 430074, China
Corresponding authors: (18571751983@163.com).

Abstract Digital libraries, as information resource sharing platforms, face severe challenges of data security and copyright protection. In this paper, we propose a DCT-Schur based digital watermarking encryption scheme to realize the security protection of digital resources through the combination of discrete cosine transform, Schur matrix decomposition and Logistic chaotic mapping. The scheme constructs the watermark embedding process from six links: watermark preprocessing, DCT transform, carrier image chunking, Schur matrix decomposition, watermark feature embedding and carrier image restoration, and controls the extraction and decryption restoration of watermarked signals through key sequences. The experimental results show that the scheme has good invisibility, and the PSNR values of the images after embedding the watermark are all greater than 45.0 dB, and the SSIM coefficients are all more than 0.993. In terms of robustness, the scheme can effectively resist all kinds of attacks, and the NC value of the extracted watermark still reaches 0.9663 even under the attack of rotating 10°; the NC value under the attack of shearing 1/4 stays above 0.9908, which is significantly better than the existing methods. This scheme performs well in balancing watermark invisibility and robustness against attacks, and provides an effective solution for data security design and copyright protection in digital libraries.

Index Terms Terms digital library; data security, copyright protection, discrete cosine transform, Schur matrix decomposition, digital watermarking

I. Introduction

In today's highly informatized era, digital libraries have become an important channel for people to obtain information and disseminate knowledge. Digital libraries have many advantages such as large information storage, fast dissemination speed, wide coverage, etc., and have gradually become an important platform for people to obtain information, learn knowledge and communicate and interact with each other, providing people with more convenient and efficient information services [1]-[3]. However, while digital libraries bring convenience and efficiency to people, they also face many security challenges. Since the operation of digital libraries is highly dependent on information technology infrastructure such as computers and networks, they face more complex security risks [4]. The digital library network system is characterized by open architecture, wide distribution, resource sharing and network utility, which enhances the practicality and at the same time increases the vulnerability of the system, providing opportunities for virus damage, hacking and phishing [5]-[8]. From the data storage point of view, the current digital library servers, PCs commonly used operating system software is mainly windows 7, windows 2003 Server and linux. Strictly speaking, these software are more or less technical defects or storage vulnerabilities, virus resistance ability is low, directly affecting the security of data [9]-[12]. Once the digital library network system suffers damage, resulting in the loss of important data, the consequences will be unimaginable. Therefore, how to protect the data security of digital libraries has become a digital library development process, the need to urgently solve the problem.

Digital libraries, in addition to data security risks, there is also the risk of copyright disputes. Digital library copyright refers to the process of digitizing users' content information and digital resources in carrying out digital services by libraries. When carrying out digital services, libraries need to obtain authorization from the content copyright holder to edit, integrate and process the content of the work, and finally present it to readers in digital form [13], [14]. In addition, libraries can also protect the copyright of relevant content by purchasing the copyright [15]. When managing the digital copyright of the library, it is necessary to carry out the process of copyright registration, work authorization, etc. In the traditional copyright management, there are only two main parties, the right holder and the management agency, in which case the management agency can carry out unified management of the work [16]-[18]. In the digital library to carry out digital services, the user is not direct access to the work, its content of the work does not have any decision-making power, in order to prevent users from illegal use of digital resources, the need to authenticate its content and identity [19]. For the authentication problem, cryptography principles can be used to realize [20]. As it is necessary to determine the content such as the identity information and authorization information of the author or user when carrying out digital services in libraries. Therefore, the current copyright management methods still have some limitations. And in the field of information security, encryption algorithms are widely used to protect the confidentiality, integrity and reliability of data, which is an effective way to design data security and copyright protection in digital libraries [21], [22].

With the rapid development of information technology, digital libraries have become an important platform for knowledge acquisition and dissemination, in which a large number of digital resources are stored to provide users with convenient access to information. However, the easy-to-replicate and easy-to-distribute nature of digital resources has also brought about serious data security and copyright protection problems. Digital products such as images, music, videos and animations in digital libraries are frequently subject to infringement, piracy and tampering, which not only jeopardizes the legitimate rights and interests of copyright owners, but also affects the healthy development of digital libraries. Although traditional encryption technology can protect data security to a certain extent, it is difficult to provide continuous copyright protection during the use of resources. Therefore, it becomes extremely important to explore the data security and copyright protection technologies suitable for the digital library environment. Digital watermarking technology, as a method to hide copyright information in digital carriers with the characteristics of invisibility, robustness and security, has become an effective means to solve the problem of digital copyright protection. However, the existing digital watermarking algorithms still have limitations in resisting geometric attacks such as rotation and shear, and their robustness needs to be improved. Based on this, this paper combines the mathematical properties of discrete cosine transform and Schur matrix decomposition, and introduces Logistic chaotic mapping to enhance security, and proposes a data security and copyright protection scheme designed for digital libraries. The discrete cosine transform can efficiently concentrate the image information to the low-frequency coefficients, which is convenient for watermarking in the frequency domain, the Schur matrix decomposition has the advantages of small computation and good stability, and its decomposed diagonal elements are relatively stable to the perturbation, which is suitable for embedding the watermarking information, and the Logistic chaotic mapping provides a good randomness and security guarantee for the encryption of watermarking. The scheme in this paper constructs a complete watermark embedding and extraction process through the organic combination of these three techniques. In the watermark embedding process, the watermark image is first pre-processed with chaotic encryption, then the carrier image is processed with DCT transformation and chunking, then each chunk is decomposed by Schur and the appropriate position is selected to embed the watermark signal, and finally the carrier image is restored. In the process of watermark extraction, the embedding position is localized by the key sequence, and the watermark feature signal is extracted and then decrypted and restored. This multi-level technology fusion not only improves the invisibility of the watermark, but also enhances the resistance to various types of attacks, especially the robustness to geometric attacks. In this paper, we will verify the effectiveness of this scheme through a large number of experiments and compare and analyze it with the existing methods, so as to provide theoretical support and technical reference for digital libraries to build a safe and reliable data protection framework.

II. Data security and copyright protection technologies for digital libraries

At present, digital products of digital libraries are infringed, pirated and arbitrarily tampered with from time to time. On the basis of strengthening the network information security of digital libraries, we can effectively do a good job of copyright protection of digital products by actively combining the use of traditional copyright protection technology with digital watermarking technology.

II. A.Data security technologies

Data security techniques for digital libraries include encryption, authentication techniques, anti-virus techniques and firewall techniques. In this paper, encryption algorithms are mainly utilized to realize the design of data security in digital libraries.

II. A. 1) Encryption

There are various encryption methods, generally using information transformation rules to turn plaintext information into ciphertext information. It can encrypt both transmission information and storage information, turning computer data into a pile of messy data, and even if the attacker gets the encrypted information, it is just a string of meaningless characters. Encryption can effectively counter threats such as interception and illegal access.

II. A. 2) Authentication techniques

Authentication in computer networks mainly includes digital signatures, identity authentication and digital proof. The digital signature mechanism provides a method of identification, and the authentication mechanism provides a method of recognizing and confirming the true identity of both parties to an exchange of information, which can be used as the basis for access control. Authentication must be able to recognize each other accurately and should also provide two-way authentication, i.e., mutual proof of identity. Proof of identity is sometimes called "proof of public key" or "digital ID", "digital passport".

II. A. 3) Anti-virus technology

The usual anti-virus technology can be divided into three kinds: virus prevention technology, virus detection technology and virus removal technology. The network system should form a unified and complete virus defense system, and the library network administrators should also regularly upgrade the hardware and software firewalls, as well as update the virus database of the anti-virus software. Anti-virus software is used to prevent viruses from the Internet from entering the interior.

II. A. 4) Firewall technology

Firewalls achieve effective management of network security by controlling and monitoring information exchange and access behavior between networks, and their basic functions are: filtering data into and out of the network, managing access behavior into and out of the network, blocking certain prohibited behaviors, recording information content and activities through the firewall, and detecting and alerting network attacks.

II. B.Applications of digital watermarking

With the development of digital technology, digital watermarking technology has become one of the effective ways to realize the protection of intellectual property rights, but also an important technical means of network information security. The application of digital watermarking technology in the copyright protection of digital libraries is shown in Figure 1, which mainly has four important applications, such as access and use rights control, intellectual property protection of digital products, protection of important labeling information, tampering tips and integrity protection.

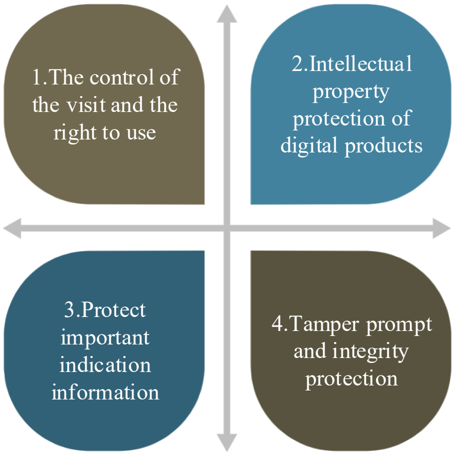
1.The control of the visit and the right to use
2.Intellectual property protection of digital products
3.Protect important indication information
4.Tamper prompt and integrity protection

Figure 1: The application of digital watermarking in copyright protection of digital library

II. B. 1) Control of access rights

Digital library digital product resources face a large number of service users, different levels of users in the use of digital product resources should have different permissions, i.e., different use of different permissions have different scope of resource utilization. Generally can be added to the resources in the digital watermark to control the use of the user's resources permissions.

II. B. 2) Digital Intellectual Property Protection

Digital products such as images, music, videos and animations in digital libraries are very easy to reproduce, copy and modify, so copyright protection of digital products is increasingly important. Digital libraries can use digital watermarking technology to protect intellectual property by embedding watermarks into the library's resources. Digital watermarking utilizes the principle of data hiding to make the copyright symbol invisible or inaudible, which can achieve the purpose of protection without damaging the original work.

II. B. 3) Protection of important labeling information

In digital libraries, some data such as remote sensing image data with labeling information (e.g. date, time, latitude, longitude, etc.) are often more important than the data itself and have more confidentiality value. And some data without labeling information sometimes can not be used, but the labeling information directly marked on the original data is not safe. Digital watermarking technology provides a way to hide the marking, marking information can not be seen on the original data, only through a special program can be read and extracted.

II. B. 4) Tamper alerts and integrity protection

An important branch of digital watermarking is fragile watermarking, which protects the integrity of a digital product. Vulnerable watermarks are obtained from the original data of a digital work by a hash function and are hidden in publicly released digital works. A tampering attack on digital media such as images and sounds will destroy the vulnerable digital watermark. The integrity checker can determine whether the original data has been tampered with by reading the watermark in the digital product.

III. DCT-Schur based digital watermarking encryption scheme

Based on the above elaboration of data security and copyright protection techniques for digital libraries, this paper proposes a digital watermark encryption scheme based on DCT-Schur to guarantee the data security and copyright protection of digital libraries.

III. A. Discrete cosine transform

The discrete cosine transform (DCT) is a mathematical operation closely related to the Fourier transform. In the Fourier series expansion, if the expanded function is an even function, then its Fourier series contains only the cosine term, and then its discretization can derive the cosine transform, so it is called the discrete cosine transform. In data compression, the DCT transform is a commonly used coding method with fast computation speed, which is very suitable for image compression and random signal processing.

III. A. 1) One-dimensional discrete cosine transforms

The one-dimensional finite-length discrete sequence $f(i)$, $0 \le i \le N-1$ is described by $f = \{f(i), 0 \le i \le N-1\}$. f of the one-dimensional discrete cosine transform (1D-DCT) $F = \{F(u), 0 \le u \le N-1\}$:

$$F(u) = a_u \sum_{i=0}^{N-1} f(i) \cos\left[\frac{(2i+1)u\pi}{2N}\right] \tag{1}$$

$$f(i) = \sum_{i=0}^{N-1} a_u F(u) \cos\left[\frac{(2i+1)u\pi}{2N}\right] \tag{2}$$

where coefficient a_u is defined:

$$a_u = \begin{cases} \sqrt{1/N} & u = 0 \\ \sqrt{2/N} & u = 1, 2, \cdots, N-1 \end{cases} \tag{3}$$

III. A. 2) Two-dimensional discrete cosine transforms

The two-dimensional finite-length discrete sequence $f(i,k), 0 \le i \le N_1 - 1, 0 \le k \le N_2 - 1$ is denoted by $f = (f(i,k), 0 \le i \le N_1 - 1, 0 \le k \le N_2 - 1)$. The two-dimensional discrete cosine transform (2D-DCT) $F = \{F(u,v), 0 \le u \le N-1, 0 \le v \le N-1\}$ of f is defined as:

$$F(u,v) = a_u a_v \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} f(i,k) \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2k+1)v\pi}{2N}\right] \tag{4}$$

$$f(i,k) = \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} a_u a_v F(u,v) \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2k+1)v\pi}{2N}\right] \tag{5}$$

The definition of coefficient a_u, a_v is the same as equation (3).

The two-dimensional discrete cosine transform can concentrate the main information of the image into the least number of low-frequency coefficients, and cause the smallest image “block effect”, which can realize a good compromise between the computational complexity and the ability to concentrate the information, so it is widely used in lossy compression.

III. A. 3) Three-dimensional discrete cosine transforms

The three-dimensional finite-length discrete sequence $f(i,k,l), 0 \le i \le N_1 - 1, 0 \le k \le N_2 - 1, 0 \le l \le N_3 - 1$ is denoted by $f = (f(i,k,l), 0 \le i \le N_1 - 1, 0 \le k \le N_2 - 1, 0 \le l \le N_3 - 1)$ denotes. The 3D-DCT transform $F = \{F(u,v,t), 0 \le u \le N-1, 0 \le v \le N-1, 0 \le t \le N-1\}$ of f is defined as:

$$\begin{gathered} F(u,v,t) = a_u a_v a_t \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} f(i,k,l) \\ \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2k+1)v\pi}{2N}\right] \cos\left[\frac{(2l+1)t\pi}{2N}\right] \end{gathered} \tag{6}$$

$$\begin{gathered} f(i,k,l) = \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} a_u a_v a_t F(u,v,t) \\ \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cos\left[\frac{(2k+1)v\pi}{2N}\right] \cos\left[\frac{(2l+1)t\pi}{2N}\right] \end{gathered} \tag{7}$$

The defining equation of the coefficient a_u, a_v, a_t in Eq. is the same as Eq. (3). In this paper, digital watermarking techniques for digital libraries are investigated based on still images, and thus the two-dimensional DCT transform method is used.

III. B. Schur decomposition

Matrix Schur decomposition is one of the basic decomposition methods for matrices, which is specified as follows:

Let the matrix $A \in C^{n\times n}$, then there exists a You matrix $U \in C^{\pi\times n}$ and an upper triangular matrix $T \in C^{n\times n}$ such that $A = UTU^H$ and the main diagonal elements of T are the eigenvalues of A. where U^H denotes the conjugate transpose of U.

Corollary If A is a real symmetric matrix, then there exist orthogonal matrices Q and diagonal matrices T such that $A = QTQ'$ and the main diagonal elements of T are the eigenvalues of A.

For any real square matrix, there is the following matrix splitting theory:

Any real square matrix A can be uniquely represented as the sum of a symmetric matrix B and an antisymmetric matrix C, i.e., $A = B + C$. where:

$$B = \frac{1}{2}(A + A'); \quad C = \frac{1}{2}(A - A') \tag{8}$$

Assuming that the diagonal matrix obtained by Schur decomposition of the symmetric matrix B determined after splitting A is T, the change $\delta\lambda$ in the diagonal elements (i.e., the eigenvalues of B) of T when applying a perturbation to the matrix A to obtain $A + \delta A$ satisfies the inequality:

$$|\delta\lambda| \le \|\delta B\|_2 \le \frac{1}{2}\|\delta A + (\delta A)'\|_2 = \|\delta A\|_2 \tag{9}$$

where δB represents the perturbation of the symmetric matrix B and $\|\cdot\|_2$ denotes the 2-parameter of the matrix. The significance of the above equation is that when a perturbation δA is applied to a matrix A to obtain $A + \delta A$, the perturbation $\delta\lambda$ of the diagonal elements of the decomposed T does not exceed the 2-parameter of the perturbed matrix δA.

Since the grayscale image can be regarded as a real matrix, and noting that the diagonal elements of T are relatively stable compared to the perturbations of the image square matrix A, the watermarking information is considered to be embedded in the diagonal elements of T with the largest absolute value, and the algorithm is robust according to the above conclusion. In addition, according to the theory of Schur decomposition of matrices, the computation of Schur decomposition is much smaller than that of singular value decomposition. Therefore, by applying the theory of Schur decomposition of matrices to the field of digital watermarking, the algorithm is not only robust, but also fast in computation.

III. C. Logistic Chaos Mapping

Chaos occurs in rational systems with nonlinear processes sensitive to starting and control points, which are random and unpredictable in chaotic orbits. This security system is characterized as random, hybrid and reliable. Therefore, the most common approach is to use chaotic systems for cryptography.

The one-dimensional Logistic mapping is calculated as Eq:

$$x(k+1)=\mu x(k)[1-x(k)],(k=0,1,\cdots n) \tag{10}$$

where the initial value x_θ takes the value range of (0, 1) and μ is called the Logistic parameter and takes the value range of [0, 4]. Only when x_θ takes values in the range (0, 1) and μ takes values in the range (3.5699456, 4], and especially the closer the value of μ gets to 4, the values generated by the iterations are pseudo-randomly distributed states.

III. D. Watermark Embedding Algorithm Design

The watermark embedding algorithm design is divided into six components, which are preprocessing stage, DCT discrete cosine transform, carrier image chunking, Schur matrix decomposition, watermark feature good embedding, and carrier image restoration.

III. D. 1) Embedding Preprocessing

(1) Watermark preprocessing

In order to ensure the security of watermark embedding, the watermark image needs to be preprocessed before embedding the image. Therefore, the image encryption algorithm based on chaotic mapping is used. After inputting the initialization control parameters X_0,r,α,b,c, and using the Logistic Chaotic Key Generator to obtain the chaotic key sequence X_n, the watermark image is encrypted to generate the color encrypted image WM.

(2) Carrier image and watermark image reading

Read the color carrier image P and the color watermark image WM to convert the representation of WM through Fibonacci and Logistic preprocessing to obtain the ciphertext image and then the type of the ciphertext is converted to the pixel value into a binary watermarking signal, which provides binary key sequences for the subsequent embedding of the watermark.

III. D. 2) DCT Discrete Cosine Transform

The read-in color carrier image P is processed by 2D-DCT (Discrete Cosine Transform) algorithm. After acquiring the color image P, it is necessary to first perform a three-channel color stripping of the image to separate it into three color channel components RGB, and then, according to the 2D discrete cosine formula, perform a 2D-DCT transform on each channel component to obtain P_R,P_G,P_B.

III. D. 3) Carrier image chunking

In order to disperse the embedding of the watermark feature signal points, the carrier image needs to be cut into a number of equal-proportional chunks, and each image chunk is embedded with a watermark feature signal value. According to the pixel ratio comparison between the color image to be embedded with the watermark signal and the original color watermark image, calculate the image chunk size and the number of chunks to be divided and perform disjoint matrix chunking $Block_{x,y}$ (x,y denotes the y th matrix chunk of the x th color channel, $x\in\{R,G,B\}$). The carrier image chunk size is set to 4×4, which effectively improves the selectivity of watermark embedding, thus weakening the visual impact of watermark embedding and enhancing the invisibility of the algorithm.

III. D. 4) Schur matrix decomposition

Schur matrix decomposition is a necessary operation before watermark embedding, by performing Schur matrix decomposition for each image chunk $Block_{x,y}$, the You matrix $U_{x,y}$ and the upper triangular matrix $T_{x,y}$ are obtained as shown in Equation (11):

$$\left[U_{x,y},T_{x,y}\right]=Sch\ ur(Block_{x,y}) \tag{11}$$

In this paper, we mainly work on the watermark embedding of the upper triangular matrix $T_{x,y}$, by embedding the selection of the upper triangular matrix $T_{x,y}$ and modifying the value of a certain position, we have achieved the purpose of the embedding of watermarked feature signals.

III. D. 5) Watermark feature signal embedding

(1) Embedded watermark chunk selection

Using a square color watermark image with a resolution of 32, the watermark image is converted to binary with a total of 8192 bit. Embedding them into the color carrier image respectively, 8192 chunks need to be screened in each component for embedding. This algorithm adopts the idea that the upper triangular matrix $T_{x,y}$ obtained by Schur decomposition of 16384 carrier image chunks is used to summarize the maximum value of $T_{x,y}$ on the diagonal of $T_{\max}$ and find the average value of T_{avg}. After obtaining T_{avg} and all carrier image chunks of $T_{\max}$ for size judgment, after meeting the conditions, the matrix T for watermarking signal embedding, and record the selected embedding sequence, and the final output is the Key key, this key is the key sequence of watermark extraction.

(2) Watermark embedding

Let the watermark embedding strength be Q, the watermark signal to be embedded is judged as follows: (a) When the watermark feature signal to be embedded is 1 bit, then $T=\left\lfloor \frac{T_{\max}}{Q} \right\rfloor Q+\frac{3}{4}Q$. (b) When the watermark signal to be embedded is 0bit, then $T=\left\lfloor \frac{T_{\max}}{Q} \right\rfloor Q+\frac{1}{4}Q$.

III. D. 6) Carrier Image Reduction

(1) Inverse Schur matrix decomposition

The inverse Schur decomposition is performed on all the chunks $Block_{x,y}$ of the carrier image to generate the image chunks $Block_{x,y}{}'$: $Block_{x,y}{}'=U_{x,y}\times T_{x,y}\times U_{x,y}^{T}$, where the symbol "$T$" in $U_{x,y}^{T}$ denotes the transpose operation of the matrix.

(2) Three-channel synthesis of color images containing watermarks

Embed the watermark feature signal into the upper triangular matrix of the image, and then inverse decomposition reduction, the three color channel components R',G',B' for the channel merger, to get the watermarked color image with watermarks P', to complete the embedding of the watermark feature signal. This completes the embedding of the watermarked feature signal.

III. E. Watermark Extraction Algorithm Design

The design of watermark embedding algorithm is divided into three parts, which are watermark image reading and splitting, watermark feature signal extraction, and watermark signal decryption and restoration.

III. E. 1) Watermark Image Read Split

(1) Watermarked color image reading

After reading the color image P embedded with the watermarked signal, it is necessary to perform a three-channel color stripping of the image first, separating it into three color channel components P_R,P_G,P_B, and then perform a DCT discrete cosine transform of the three-channel components, and use the 2D-DCT (discrete cosine transform) algorithm to perform a DCT discrete cosine transform on the color images of the watermarked signals P_R,P_G,P_B.

(2) Three-channel matrix splitting

The three color channel components P_R,P_G,P_B are subjected to matrix splitting, and according to the method used in the original embedding of the watermark, the whole split-channel image is split into multiple 4×4 scale-sized matrix blocks $Block_{x,y}{}'$, and all the matrix blocks $Block_{x,y}{}'$ are sequentially sorted for subsequent matrix decomposition.

III. E. 2) Watermark feature signal extraction

The accuracy of watermark feature signal extraction is related to the intensity Q set at the time of watermark embedding, the larger the intensity Q set, the higher the accuracy of the extracted watermark feature signal. The watermark feature signal extraction is divided into two parts:

(1) Watermark-containing signal matrix selection

According to the key sequence Key generated during the watermark embedding, the matrix sequence is selected, and Schur matrix decomposition is performed on each selected matrix chunk $Block_{x,y}{}'$ to obtain the You matrix $U'_{x,y}$ and the upper triangular matrix $T'_{x,y}$.

(2) Watermark feature signal extraction

The eigenvalues of the upper triangular matrix $T'_{x,y}$ are analyzed to find the maximum value $T_{\max'}$ on the diagonal elements of the matrix $T'_{x,y}$, and then the judgment of extracting 1bit watermark signals is carried out for each selected image chunk, and the extraction method is shown in Equation (12):

$$Bit = \begin{cases} 1, \mathrm{mod}\left(T_{\max} (\frac{Q}{2}) \right) \\ 0, \mathrm{otherwise} \end{cases} \tag{12}$$

The extracted watermark feature signals are converted to convert the binary ciphertext to be saved as a sequence of decimal ciphertexts.

III. E. 3) Watermark signal decryption restoration

The watermark signal decryption reduction is divided into two parts:

(1) Logistic chaotic mapping decryption

Use the Logistic Chaotic Key Generator to obtain the corresponding X_n of the chaotic key sequence and perform decryption operation with the decimal ciphertext sequence to generate the ciphertext sequence A.

(2) Fibonacci permutation reduction performs inverse Fibonacci permutation on each component of the ciphertext sequence, and then combines the decrypted three-channel images to obtain the final extracted color watermark image WM'.

IV. Experimental results and analysis

IV. A. Main performance indicators

The basic design requirements of digital image watermarking are as follows: (1) invisibility. That is, to make embedded watermarks lead to the transformation of the carrier data for the human eye is imperceptible, the best state is to contain watermarks between the image and the original carrier image looks the same, which is also the most basic requirements of the watermarking algorithm. (2) Robustness. That is, the digital watermark will not be easily eliminated. (3) Security. The digital watermark must withstand a variety of intentional attacks and be difficult for others to copy and forge. (4) Efficiency. The watermark extraction algorithm must be efficient, while the extracted watermark must be able to clearly identify the copyright owner. (5) Resistance to change. Unlike robustness against vandalism, resistance to inviolability means that once the watermark is embedded, it is difficult for an attacker to change or forge it.

In this paper, the watermarking algorithm utilizes Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) to evaluate the invisibility and robustness of the watermarking algorithm, and Normalized Correlation Coefficient (NC) to measure the difference between the original watermarked image and the extracted watermarked image.

The unit of PSNR is decibel (dB), the larger the PSNR value, the higher the image quality, i.e., the smaller the difference between the two images that can be seen by the naked eye.SSIM is an objective indicator to measure the similarity of two images, its value range is [0,1], the closer to 1, indicating that the watermarked image quality is better, equal to 1 can be said that the two images are completely equal. The normalized correlation coefficient (NC) becomes an objective index that provides a metric between the images and can be used to measure the similarity of the images.The value range of NC is the same as that of SSIM, which is also [0,1], and the closer the value is to 1, the higher the similarity between the images, and when it is equal to 1, it can be said that these two images are exactly the same.

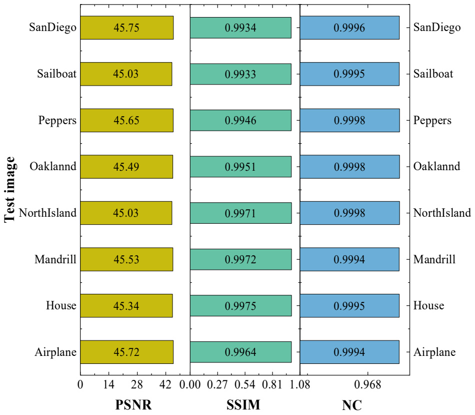

Figure 2: The PSNR value and SSIM coefficient of the embedded watermark

IV. B. Invisibility analysis

In this paper, eight color images of size 512×512 were selected as carrier images for the experiment, namely “Airplane”, “House”, “Mandrill”, “NorthIsland”, “Oaklannd”, “Peppers” and “Sailboat”, “SanDiego”, and a grayscale image with pixel size of 64×64 is selected as the watermark image for the experiment. The PSNR values and SSIM coefficients of the images after embedding the watermark are given in Fig. 2. The PSNR values of these embedded watermarked images are more than 45.0 dB and the SSIM coefficients are more than 0.993. The NC values of the extracted watermarked images and the original watermarked images are above 0.999, which is very close to 1. Therefore, from the experimental results the proposed DCT-Schur based digital watermarking encryption scheme is effective and feasible in terms of invisibility.

IV. C. Watermark Robustness Analysis

Table 1 shows the results of watermark detection in case the image is added to different types and strengths of attacks, the experimental attacks are mainly add noise, JPEG, scaling, rotation, etc., and the peak signal-to-noise ratio PSNR and normalized correlation coefficient NC are used to illustrate the quality of the image after the attack. From the experimental results, the watermark can still be effectively extracted when the image is attacked, and the PSNR of the extracted watermark is 12.64~50.85dB, and the algorithm in this paper has good robustness against conventional attacks. Comparatively, the NC values are above 0.99 for images subjected to shear attack. When the image is attacked by a larger range of rotation, the NC value is also higher, above 0.95, and the algorithm in this paper has a stronger robustness to resist rotation and shear attacks.

Table 1: Watermarking detection results under attack

Attack type	PSNR	NC
Gaussian noise 0.01	27.52	0.9982
Gaussian noise 0.05	22.81	0.9956
Pepper salt noise 0.01	30.22	0.9985
Pepper salt noise 0.05	25.62	0.9975
Zooming 1/2	36.63	1.0000
Zooming 2	50.85	1.0000
JPEG(10)	32.35	0.9981
JPEG(30)	38.48	0.9989
JPEG(50)	40.06	0.9993
Upper left corner shear 1/16	39.11	0.9976
Upper left corner shear 1/8	20.55	0.9959
Upper left corner shear 1/4	15.69	0.9908
Center shear 1/4	14.73	0.9988
Rotations 1°	20.71	0.9973
Rotations 3°	17.08	0.9896
Rotations 10°	14.95	0.9663
Rotations 30°	12.64	0.9558

IV. D. Comparative Experimental Analysis

In order to further verify the effectiveness of this paper's algorithm, this paper's DCT-Schur digital watermarking encryption algorithm is compared with two digital watermarking encryption algorithms, and the results of the comparison experiments are shown in Table 2.Method 1 adopts the YCbCr color space, combines the wavelet transform with the singular value decomposition to construct the feature matrix to generate the zero watermark. Method 2 performs wavelet transform on the image, chunks its low-frequency subbands and SVD decomposes it, and constructs the zero watermark using singular values and random sequences.

The DCT-Schur digital watermarking encryption algorithm in this paper has a general advantage in resisting noise, JPEG compression, deflation, shear, rotation and other attacks, especially the advantage of resisting shear attack and rotation attack is more obvious, and the NC value under various attacks is still maintained above 0.9. Fig. 3 and Fig. 4 show the comparative effects of the two methods during rotation and shear attacks, respectively. In Fig. 3, when the rotation angle varies from 1° to 170°, the NC values of this paper's DCT-Schur method are all significantly better than those of the comparison methods, and its overall average value reaches 0.923, while the overall average values of Method 1 and Method 2 are 0.810 and 0.774. In Fig. 4, when the shear position and size vary, the NC values of this paper's DCT-Schur method are all significantly better than Method 1 and Method 2, with an average NC value of 0.983, while the average NC values of the comparison methods are all below 0.93.

The analysis shows that the digital watermarking encryption algorithm based on DCT-Schur proposed in this paper can effectively resist different digital signal processing attacks, has good performance in all aspects of performance, and can be used in data security protection and copyright protection in digital libraries.

Table 2: Comparison experiment results

Attack type	Method 1	Method 2	DCT-Schur
Pepper salt noise 0.01	0.9977	0.8915	0.9990
Pepper salt noise 0.05	0.9953	0.8906	0.9986
Zooming 1/2	0.9965	0.9985	1.0000
Zooming 2	0.9947	0.9954	1.0000
JPEG(10)	0.9915	0.8718	0.9975
JPEG(50)	0.9977	0.8805	0.9987
Upper left corner shear 1/16	0.9586	0.8378	0.9974
Upper left corner shear 1/4	0.8945	0.8524	0.9914
Center shear 1/4	0.8971	0.7948	0.9662
Rotations 10°	0.8559	0.7948	0.9567
Rotations 30°	0.7934	0.8175	0.9215
Rotations 50°	0.7644	0.7791	0.9018

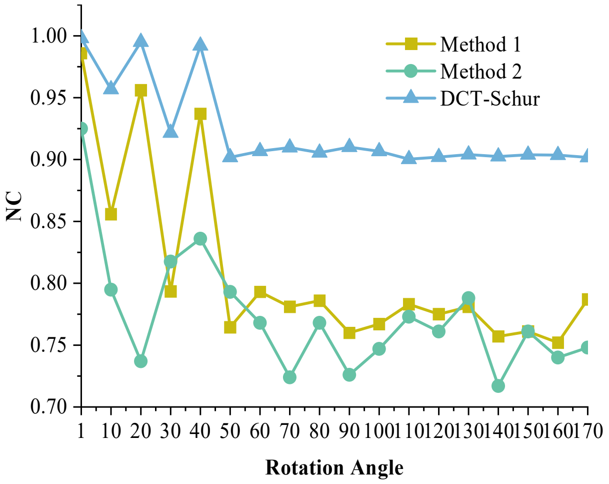

Figure 3: The comparison effect of the three methods of rotating attack

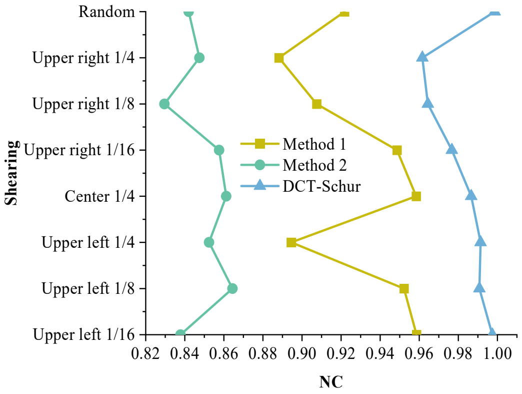

Figure 4: The contrast effect of the three methods of shear attack

V. Conclusion

The DCT-Schur based digital watermark encryption scheme proposed in this paper successfully solves the problem of data security and copyright protection in digital libraries. The experimental results show that the scheme has strong anti-attack ability while guaranteeing the invisibility of the watermark. In terms of invisibility, the PSNR values of eight different carrier images embedded with watermarks exceed 45.0dB, the SSIM coefficient remains above 0.993, and the NC values of the extracted watermarks and the original watermarks reach above 0.999, which makes the watermarks have almost no effect on the visual effect of the original image. In terms of robustness, even under severe attacks such as Gaussian noise of 0.05, JPEG compression quality factor of 10, 1/4 shear in the upper corner, and rotation of 30°, the NC values of the extracted watermark still reach 0.9956, 0.9981, 0.9908, and 0.9558, respectively, which are excellent. Compared with the comparison methods, this scheme achieves an average NC value of 0.923 in resisting rotation attack, which is higher than that of 0.810 in Method 1 and 0.774 in Method 2, and an average NC value of 0.983 in shear attack, which significantly exceeds that of 0.93 in the comparison methods.In addition, this scheme combines the preprocessing of Logistic Chaos Mapping with the Fibonacci Disruption reduction mechanism, which further improves the security of watermarking and effectively prevents unauthorized extraction and tampering. The study shows that the DCT-Schur digital watermarking algorithm has obvious advantages in balancing invisibility and robustness, and provides a feasible scheme for digital libraries to build a comprehensive data security and copyright protection framework.

References

[1] Yaqin, M. A. (2022). Strategy of library development towards digital library. Khatulistiwa: Jurnal Pendidikan Dan Sosial Humaniora, 2(2), 52-69.

[2] Li, Y., & Liu, C. (2019). Information resource, interface, and tasks as user interaction components for digital library evaluation. Information Processing & Management, 56(3), 704-720.

[3] Mehta, D., & Wang, X. (2020). COVID-19 and digital library services–a case study of a university library. Digital library perspectives, 36(4), 351-363.

[4] Magsi, I., Shaheen, N., Channar, W. A., Ali, M., Lakho, Z., & Ahmed, A. (2025). Cyber-Security Challenges in Digital Libraries. Review Journal of Social Psychology & Social Works, 3(1), 344-350.

[5] Sampathkumar, M., & Mulugu, S. D. (2020). Digital library, features, strategies, infrastructure and their benefits for users in digital era. J. Emerg. Technol. Innov. Res, 7(9), 964-975.

[6] Liu, Y. (2019). Risk and preventive strategy of network security in university digital library. In 9th International Conference on Management, Education and Information.

[7] Wu, Z., Shen, S., Li, H., Zhou, H., & Zou, D. (2021). A comprehensive study to the protection of digital library readers' privacy under an untrusted network environment. Library Hi Tech, 40(6), 1930-1953.

[8] Chickombe, D. S., & Maina, C. (2021). Vulnerabilities Facing Digital Content at the University of Nairobi and Catholic University of Eastern Africa Academic Libraries. system, 11(4).

[9] Patra, S., & Sahoo, J. (2022). A literature review on digitization in libraries and digital libraries. Preservation, Digital Technology & Culture, 51(1), 17-26.

[10] Xing, L., Zhao, L., & Zhang, J. (2022). Service Security of Cloud Storage Technology in Digital Library. In Innovative Computing: Proceedings of the 4th International Conference on Innovative Computing (IC 2021) (pp. 205-212). Springer Singapore.

[11] Huang, S., Han, Z., Yang, B., & Ren, N. (2019). Factor identification and computation in the assessment of information security risks for digital libraries. Journal of Librarianship and Information Science, 51(1), 78-94.

[12] Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science, 01655515231160026.

[13] Safaii, H., & Afshar Quchani, Z. (2016). Copyright in digital library. Comparative Law Review, 7(1), 225-251.

[14] Atalar, C. (2021). Development and Implementation of Electronic Library for Protection of Copyrights. Erzincan University Journal of Science and Technology, 14(3), 874-886.

[15] Huiming, C. (2021). Research on Limitations and Exceptions of Technical Measures for Long-term Preservation of Library Digital Resources: Considerations Based on the “Technical Path” of Copyright Protection. Libraly Journal, 40(1), 48.

[16] Eiriemiokhale, K. A. (2018). Copyright issues in a digital library environment. In Handbook of Research on Managing Intellectual Property in Digital Libraries (pp. 142-164). IGI Global.

[17] Tamilselvan, N. (2024). Blockchain-based digital rights management for enhanced content security in digital libraries. International Journal of Blockchain Technology (IJBT), 2(1), 1-8.

[18] Papi, Z. (2025). Exceptions and exemptions to copyright for libraries digital resources: Comparative study in the legal system of Iran, France, Germany and some international documents and treaties. Librarianship and Information Organization Studies, 33(1), 3-22.

[19] Fitria, E., Sabandi, A., Irsyad, I., Al Kadri, H., & Khomarudin, A. N. (2023). Digital Library Development at MAN 1 Bukittinggi as an Accessibility Convenience Support for Users. JURTEKSI (Jurnal Teknologi dan Sistem Informasi), 9(2), 133-140.

[20] Ao, W., Fu, S., Zhang, C., Huang, Y., & Xia, F. (2019, August). A secure identity authentication scheme based on blockchain and identity-based cryptography. In 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET) (pp. 90-95). Ieee.

[21] Goyal, V., & Kant, C. (2018). An effective hybrid encryption algorithm for ensuring cloud data security. In Big data analytics: Proceedings of CSI 2015 (pp. 195-210). Springer Singapore.

[22] Singh, A. K., & Kumar, C. (2020). Encryption-then-compression-based copyright protection scheme for E-governance. IT Professional, 22(2), 45-52.